AMERICAN YEARBOOK OF INTERNATIONAL LAW
ISSN: 2732-9925
Vol.3, 2024 Article 11

Impact of the General Data Protection Regulation of the European Union on the legal regime on the legal regime of international transfers of personal data

Alfonso Ortega Gimènez

DOI:10.5281/zenodo.14290236

Impact of the General Data Protection Regulation of the European Union on the legal regime on the legal regime of international transfers of personal data

DOI:10.5281/zenodo.14290236

Alfonso Ortega Gimènez, Professor of International Private Law at the Faculty of Law of the Miguel Hernández University of Elche. Vice Dean of the Degree in Law. Director of the Master UMH-ICAE. Director of the Chair of International Private Relations UMH-ICAO. Director of the Alicante Provincial Immigration Observatory. Partner Director of the Coex International Trade, Spain

Abstract: International data transfers involve a flow of personal data from Spanish territory to recipients established in countries outside the European Economic Area. It is the European Commission that decides, with effects for the whole Union, that a third country, a territory or a specific sector of a third country, or an international organisation offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union with regard to the third country or international organisation.

Keywords: Data protection; international data transfer; safeguards; supervisory authority.

Regulatory approach to international data transfers: The general data protection regulation

There is a pressing need to address two key issues. First, the cumulative and simultaneous application of different national data protection laws must cease. Second, the rules governing data export need modernization. The goal here is to facilitate the "free flow of personal data" and ensure the protection of data subjects' right to data privacy, especially in instances of unlawful international data transfers.

It is therefore necessary to improve the current mechanisms for international data transfer to third states by including adequacy decisions (i.e. decisions certifying the adequacy of third states' data protection rules), as well as appropriate safeguards (such as standard contractual clauses or binding corporate rules) to ensure a high level of protection in international data processing operations and to facilitate the cross-border flow of data. In short, it is about rebuilding the legal framework in order to consolidate it with a modern, solid, coherent and comprehensive data protection framework for the EU and for third states. A robust and unified legislative framework aims to strengthen the single market aspect of data protection. This framework

eliminates varying levels of protection across EU Member States caused by disparities in their legal, regulatory, and administrative provisions, ultimately fostering stronger commercial ties between the European Union and third countries.

In this context, the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) of 25-01-2012[1] (hereinafter, General Data Protection Regulation or GDPR) emerges, a general and directly applicable rule without the need for transposition; the objective is clear: to achieve legislative uniformity (Solar Calvo, 2012), simplifying the legal regime on international data transfers.

The system of adequacy decisions

Transferring personal data to third states with adequate protection requires a Commission decision. This is a key element for considering international transfers valid. Article 45 lays down the criteria, conditions and procedures for the adoption of an adequacy decision by the Commission, based on Article 25 of Directive 95/46/EC. The criteria to be taken into account for the Commission's assessment of whether or not an

1COM (2012) 11 final.

adequate level of protection exists expressly include:

The Article now explicitly confirms the possibility for the Commission to assess the level of protection afforded by a territory or a processing sector in a third country. For transfers to third countries for which no adequacy decision has been taken by the Commission, Article 46 requires appropriate safeguards to be provided, notably standard data protection clauses, binding corporate rules and contractual clauses. The option to use the standard data protection clauses provided by the Commission relies on Article 26(4) of Directive 95/46/EC. As a novelty, these standard data protection clauses can now also be adopted by a supervisory authority and declared generally valid by the Commission. Binding corporate rules are now specifically mentioned in the legal text. The option of contractual clauses offers some flexibility to the controller or processor, but is subject to prior authorisation by the supervisory authorities.

In this regard, the approval procedure according to (Recital 103) states that:

The Commission may decide, with effect for the whole Union, that a third country, a territory or a specific sector within a third country, or an international organisation offers an adequate level of data protection, thereby providing throughout the Union legal certainty and uniformity as regards the third country or international organisation which is considered to offer such a

level of protection. In such cases, transfers of personal data to these countries can take place without any further authorisation being required. The Commission may also decide to revoke such a decision, subject to prior notice and a fully reasoned statement to the third country or international organisation.

This shows the Commission's absolute leading role in taking the decision on adequacy, and it will do so through the opinions of the committees, such as the European Data Protection Committee. Another issue, before listing the elements to be taken into account, is to determine who is subject to assessment - not only third states are subject to assessment, but also companies that do not provide an adequate system of protection; on the other hand, in order to assess the level of protection, the Regulation establishes that the following aspects shall be taken into account.

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including legislation relating to public security, defence, national security and criminal law, and access to personal data by public authorities, as well as the application of such legislation, data protection rules, professional standards and security measures, including rules on on onward transfers of personal data to another third country or international organisation observed in that country or international

organisation, case law;

(b) the existence and effective functioning of an independent supervisory authority or authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights, and for cooperating with the supervisory authorities of the Union and of the Member States. At this point, it is very important, as required by Recital 104, that the supervision is truly independent.

(c) international commitments entered into by the third country or international organisation concerned, or other obligations arising from legally binding agreements or instruments.

It is foreseen that the decision will be reviewed every four years with the objective of monitoring whether the third country continues to comply with these conditions. If it is found that such a standard is no longer met, the Commission will repeal, suspend or amend the agreement. Discussions will be initiated with that state to remedy the previous situation. Transfer to third parties is also allowed even in the absence of a decision, but with sufficient guarantees, such as the adoption of binding instruments.

The main consequence of the adoption of an adequacy decision is found in Article 45(1) of the Regulation, that a transfer of personal data to a third country or international organisation may take place, and that such a transfer does not require any specific authorisation.

Transfers by means of adequate safeguards

Transfers using adequate safeguards are crucial when adequacy decisions are absent. This is why the Regulation strengthens the rules, building on Directive 95/46/EC's foundation. In Regulation recital 108, there are indications of the importance of this requirement: Those safeguards must ensure the observance of data protection requirements and data subjects' rights appropriate to processing within the Union, including the availability to data subjects of enforceable rights and effective legal remedies, including the right to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country.

If a decision according to the above features has not been issued, personal data may only be transferred to a third State or organisation if adequate safeguards and enforceable rights have been provided. Here the GDPR establishes two types of adequate safeguards; those that require authorisation and those that do not.

A) Guarantees without requiring authorisation are:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules;

(c) standard data protection clauses adopted by the Commission or supervisory authority and approved by the Commission;

(d) a code of conduct, together with binding and enforceable commitments of the controller or processor in the third country to implement appropriate safeguards, including on the rights of data subjects and approved by the supervisory authority; or

e) a certification mechanism, with the same commitments as the previous measure. The mechanism is voluntary, and will be issued by a body accredited by the DPA or by the authority itself.

B) Where there is authorisation by the supervisory authority, it shall be required by;

(a) contractual clauses between the controller or processor and the controller, processor or recipient of the personal data in the third country or international organisation; or

(b) provisions to be incorporated in administrative arrangements between public authorities or bodies which include effective and enforceable rights for the persons concerned.

The standard contractual clauses are governed by Decision 2001/497/EC of 15 June 2001 on standard contractual clauses

for the transfer of personal data to a third country between controllers, as amended by Decisions 2004/915/EC and 2016/2297/EC; and Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries, pursuant to Directive 95/46/EC of the European Parliament and of the Council, as amended by Decision 2016/2297/EC.

The possibility to make use of standard data protection clauses of the Commission is based on Article 26(4) of Directive 95/46/EC. As a novelty, these standard data protection clauses can now also be adopted by a supervisory authority and declared generally valid by the Commission. Binding corporate rules are now specifically mentioned in the legal text. The option of contractual clauses offers some flexibility to the controller or processor, but is subject to prior authorisation by the supervisory authorities.

As a cautionary note, standard contract terms may face a significant challenge: the CJEU is expected to rule on their validity within the next year and a half.

Binding Corporate Rules

One of the most notable novelties introduced in the GDPR is to be found in Article 47, which refers to binding corporate rules, which establishes that

"the competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism",

which means that the set of rules approved will be binding as long as they comply with the requirements established in Article 47.1 of the Regulation, which is the one that grants such binding force.

Binding corporate rules can be defined as internal rules (such as a code of conduct) adopted by a multinational group of companies that define their overall policy with regard to international transfers of personal data within the same corporate group to entities located in countries that do not provide an adequate level of protection. They are intended for corporate groups only. These rules should have a minimum content: a)The structure and contact details of the corporate group or association of undertakings engaged in a joint economic activity and of each of its members; b) Transfers or sets of transfers of data, including the categories of personal data, the type of processing operations and their purposes, the type of data subjects concerned and the name of the third country or countries concerned; c) Its legally binding nature, both internally and externally; d) The application of general data protection principles, in particular purpose limitation, data minimisation, limited retention periods, data quality, data protection by design and by default, the basis of processing, the processing of special categories of personal data, measures to

ensure data security and requirements with regard to onward transfers to bodies not bound by binding corporate rules; e) The rights of data subjects in relation to processing and the means of exercising them, in particular the right not to be subject to decisions based solely on automated processing, including compliance profiling, the right to lodge a complaint with the competent supervisory authority and with the competent courts of the Member States, and the right to obtain redress, and, where appropriate, compensation for breaches of these rules; f) The acceptance by the controller or processor located in the territory of a Member State of liability for any breach of binding corporate rules by any member concerned not established in the Union; the controller or processor shall only be exonerated, in whole or in part, from such liability if it proves that the act giving rise to the damage is not attributable to that member; g) The way in which information on binding corporate rules is provided to stakeholders, in particular with regard to the provisions referred to in points (d), (e) and (f) and the right of information; h) The functions of any data protection officer, or any other person or entity responsible for the supervision of compliance with the CSV within the corporate group or group of undertakings engaged in a joint economic activity; j) Complaints procedures; k) The mechanisms established within the corporate group or group of undertakings to ensure verification of

compliance with the CSV, such as data protection audits and methods to ensure corrective actions to protect the data subject's rights. The results of such verification should be communicated to the DPO or similar; and to the board of directors of the company controlling a group or group of undertakings, and made available to the competent supervisory authority upon request; l) The mechanisms in place for communicating and recording changes to the standards and for notifying these changes to the supervisory authority; m) The mechanism for ensuring compliance with any member of the group or group of undertakings involves sharing the results of verifications related to the measures indicated in point (j) with the supervisory authority; n)Mechanisms for informing the competent supervisory authority of any legal requirements applying in a third country to a member of the corporate group or joint venture, which are likely to have an adverse effect on the safeguards set out in the binding corporate rules, and o)relevant data protection training for staff who have permanent or regular access to personal data.

Exceptions

Article 49 defines and clarifies the exceptions to a transfer of data on the basis of the existing provisions of Article 26 of Directive 95/46/EC. This applies in particular to data transfers

required and necessary for the protection of important public interests, for example in case of international data transfers between competition authorities, tax or customs administrations, or between services competent for social security or fisheries management. Moreover, under specific conditions, data transfers may be justified by a legitimate interest of the controller or processor. However, such transfers should only occur after a thorough assessment and documentation of the circumstances. In this context, a set of situations is established via a numerus clausus, where neither an adequacy decision nor adequate safeguards are necessary, and no authorization from supervisory authorities is required.

Although it is true that the Regulation establishes a closed list of cases, which seems to limit the situations in which they may occur, it does not seem to escape criticism, considering that the list offered by Article 49 is too broad, even in one of its paragraphs [Article 49.1.g)] it establishes that a transfer of personal data may take place even when none of the exceptions for specific situations referred to in the first subparagraph of this paragraph is applicable[2].

Article 49 lists exceptions for specific situations, including:

(a) the data subject has explicitly given his or her consent to the proposed transfer, after having been informed of the possible

2 Recitals 111 to 113 of the GDPR.

risks for him or her of such transfers due to the absence of an adequacy decision and of appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or for the performance of pre-contractual measures taken at the request of the data subject;

(c) the transfer is necessary for the conclusion or performance of a contract, in the interest of the data subject, between the controller and other natural or legal person;

(d) the transfer is necessary for important reasons of public interest; this paragraph refers to Recital 112, which lists a number of examples, in which this exception may apply, such as in the case of international exchanges of data between competition authorities, tax or customs administrations, between financial supervisory authorities, between social security or public health services, for example in the case of contacts aimed at tracing contagious diseases or to reduce and/or eliminate doping in sport.

The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised by the Union or Member State law applicable to the controller.

(e) the transfer is necessary for the formulation, exercise or defence of claims;

(f) the transfer is necessary to protect the vital interests of the

data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a public register which, under Union or Member State law, is intended to provide information to the public and is open to inspection by the general public or by any person who can show a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for inspection are fulfilled in each individual case. In situations where a data transfer cannot be founded upon the provisions outlined in Articles 45 or 46, including those governing binding corporate rules, and none of the exceptions specified in the initial section of this paragraph are applicable, the transfer may proceed provided it meets the following conditions: 1) The transfer must not be repetitive; 2) It should pertain to a limited number of data subjects; 3) The transfer should be deemed necessary to fulfil compelling legitimate interests pursued by the controller, interests that override the rights and freedoms of the data subject; 4) The controller must have conducted a comprehensive assessment of all circumstances surrounding the data transfer; and, 5) based on this assessment, the controller must establish and implement appropriate safeguards to ensure the protection of personal data. The controller shall inform the supervisory authority of the transfer. In addition to the information referred to in Articles 13

and 14, the controller shall inform the data subject of the transfer and of the compelling legitimate interests pursued.

With regard to the latter paragraph, discussed above, Article 49(2) establishes a limitation, which is that the transfer made shall not cover the totality of the personal data or entire categories of personal data contained in the register. If the purpose of the register is consultation by persons having a legitimate interest, the transfer shall only take place at the request of such persons or if they are to be the recipients[3].

The third paragraph also stipulates that subparagraphs (a), (b), and (c), as well as the second paragraph, shall not apply to activities conducted by public authorities exercising their public powers.

At this point, a certain limit is reached, quite appropriate in the author's opinion, which is laid down in the fifth paragraph, in relation to the transfer of data for reasons of public interest, which reads as follows: In the absence of a decision establishing data protection adequacy, Union or Member State law may, for important reasons of public interest, expressly set limits on the transfer of specific categories of data to a third country or international organisation. Member States shall notify such provisions to the Commission.

Finally, it provides that the controller or processor shall

34.5.2016 L 119/64 Official Journal of the European Union EN.

document in the records referred to in Article 30 the assessment and appropriate safeguards referred to in the second subparagraph of paragraph 1.

Authorisation by the supervisory authority, temporary suspension and contractual clauses

The increase in international transfers of personal data in areas such as human resources, financial services, banking, education, e-commerce, international judicial assistance or health research are now an integral part of the globalised economy (Fernàndez Lòpez, 2007). To understand the landscape of personal data protection regulation, countries can be categorised into three main groups.

The first group consists of those states where data protection legislation is currently in force and adapted to the present time (e.g. EU Member States, Argentina, Mexico, Canada or the USA); the second group consists of those countries that are actively working on their data protection legislation (e.g. some countries in the Latin American region); and[4] the third group consists of those countries where data protection legislation is

4Law No. 18331 on “Protection of Personal Data and 'Habeas Data' Action” of 11/08/2008; and its Regulatory Decree of 31/08/2009.

currently[5] lacking[6] (e.g. Russia, Malaysia, Taiwan, etc).[7] [8]

The main sectors of activity in which data exporters operate are telecommunications, energy, computer services, banking, chemicals and pharmaceuticals, and direct mail.

All these factors together show that autonomous business decisions are taking place, leading to a phenomenon of delocalisation of business activities in these sectors and countries, for which obtaining an authorisation for international data transfer is a legally necessary instrumental element.[9]

Indeed, taking into account the modality, purpose and destination of the authorised international data transfers, three interrelated phenomena emerge, emphasising the need to maximise the protection of individuals' data protection rights in the event of unlawful international data transfers:

1.The main form of transfer involves a controller located in

5Reglamento de la Ley núm. 29733 peruana de "Protección de Datos Personales" (Decreto Supremo núm. 003-2013-JUS), Diario El Peruano, Lima, Friday 22/03/2013.

6While Latin American countries have looked to the European model, they have also maintained different particularities and motivations when adopting their data protection regulations.

7Draft Law on "Protection of Privacy and Personal Data".

8Statutory Law No. 1581 of 17 October 2012, "whereby general provisions are issued for the protection of personal data".

9International data transfers serve various purposes which can be differentiated between: *a)* Those related to business management in a global context. Multinational companies require international data transfers for purposes such as the management, maintenance and technical support of information systems (especially in relation to the efficient management of human resources, customers and suppliers, as well as the provision of administrative support services in relation to these); and *b) those related to customer* service and other telephone marketing actions aimed at improving customer satisfaction, such as the centralised management of customer services. This group mainly includes the provision of customer services or *telemarketing*.

Spain, mainly dedicated to telecommunications services, transferring data to a service provider in a third country (data processor), utilising the standard contractual clauses provided for in European Commission Decision 2002/16/EC of 27 December 2001.[10]

2.The diversification of the geographical areas to which personal data is transferred: the USA continues to be the leading importer of data from Spain and Latin American countries are consolidating their position in second place (mainly Chile, Colombia, Peru, Paraguay and Uruguay). New destinations in Asia, especially India, have seen a significant rise in data transfers, which in recent years has tripled the number of files processed and is tending to become one of the main importers of personal data. Additionally, authorizations for data transfers to Morocco have increased.

3.A high percentage of the authorised transfers relate to services provided in third countries, indicating the increasing importance of offshoring activities outsourced to third countries.[11]

10*DO* 2002 L 6/52.

11From the Spanish perspective, the categories of international transfers of personal data are, in practice, of three types: *a)* Transfers of personal data derived from the optimisation of the management of resources by a company, whose parent company, whether Spanish or central, is located in a foreign country; *b)* Transfers of personal data linked to the nature of the activity or product (e.g., reservations of airline tickets or hotel reservations abroad contracted through travel agencies in Spain); and, c) Transfers of personal data aimed at improving customer service (e.g., in the cases of cases of travel agencies in Spain), b) Transfers of personal data linked to the nature of the activity or product (e.g., reservations of airline tickets or hotel reservations abroad contracted through travel agencies in Spain); and *c)* Transfers of personal data aimed at improving customer service (e.g., in cases where data

There is a need to reconcile the protection of the holder of the right to data protection resulting from an illicit international transfer of personal data, with the international circulation of personal data. This means that the regulatory rules based on the general principle of prohibiting transfers to countries that do not provide an "equivalent level of protection", as defined in Article 33.1 of the LOPD, aligning with Article 25.1 of Directive 95/46/EC and Article 23 of the EC Treaty (now Article 28 of the TFEU) (Estadella Yuste, 1996; Herràn Ortiz, 2002)[12].

Determining when a country offers an adequate level of data protection, embodying the essential core of data protection principles as defined in the LOPD, relies on Article 33.2 of the LOPD, Article 67 of the LOPD Regulations, and Instruction 1/2000. These provisions essentially mirror Article 25.2 of Directive 95/46/EC, stating that

"the adequacy of the level of protection offered by the country of destination shall be assessed (Aced Fèlez, 2005)[13] by the [Spanish] Data Protection Agency, taking into account all the circumstances of the transfer or category of data transfer. In particular, consideration shall be given to the nature of the data to be processed and the duration of the processing operation or operations envisaged, the country of origin and the country of final

processing is entrusted to a third party abroad, the management of which will enable the service provided to the customer to be more efficient).

12On the contrary, Article 25.1 of Directive 95/46/EC speaks of "adequate level of protection", showing a regrettable lack of coherence and terminological precision.

13The main elements to be assessed by the competent body - European Commission or AEPD, as the case may be - at the time of carrying out the assessment of the adequate level of protection are two: on the one hand, the guiding principles of data protection (purpose, data quality, transparency and security), where these must be identified and developed regardless of the nature of the continent of such principles; and, on the other hand, the mechanisms of effectiveness of such principles, which refer to the implementation, observation and compliance with the principles.

destination, the rules of law, general or sectoral, in force in the third country in question, the content of the reports of the Commission of the European Union, as well as the professional standards and security measures in force in those countries".

This provision will be complemented by Article 25.4 of Directive 95/46/EC, according to which, third states in respect of which the European Commission has declared the existence of such adequacy shall always be considered to offer an adequate level of protection; an extreme which is contemplated in Article 34, k), of the LOPD, when it states that the authorisation of the Director of the AEPD shall not be necessary,

"when the transfer is to a member state of the European Union, or a state in respect of which the Commission of the European Communities, in the exercise of its powers, has declared that it guarantees an adequate level of protection".[14]

The temporary suspension is established as a further guarantee for the adequate protection of personal data and to avoid the violation of the rights that individuals have over them, in the event of the possible illicit transfer of such data to a country that does not comply with the appropriate guarantees.

The international perspective of the European legal regime on the protection of personal data is an aspect to be considered in view of the future reform of Directive 95/46/EC. The increase in international transfers of personal data implies the need for states to react by restricting the unlawful capture, processing and dissemination of personal data.

14In the same sense, Article 68 of the LOPD.

There are several challenges ahead: firstly, the increase in outsourcing of processing -very often outside the EU- raises issues related to the law applicable to processing and the attribution of responsibility for processing; secondly, the need to clarify and simplify the rules applicable to international transfers of personal data in order to avoid the risk that the level of protection of data subjects provided for in a third country is judged differently from one Member State to another; thirdly, the need to strengthen the role of supervisory authorities in charge of data protection in order to improve the application of the rules in the area of international transfers of personal data; and finally, the need for a comprehensive instrument, applicable to data processing operations in all sectors and policies in the EU, to ensure an integrated approach and comprehensive, consistent and effective protection.

A strong, clear and uniform legal framework within the EU will give EU companies a global competitive advantage, as well as being a key benefit for service providers and an incentive for investors seeking optimal conditions for the location of services.

Bringing Directive 95/46/EC in line with the contemporary social and technological landscape represents a significant achievement. This alignment would not only ensure the proper operation of the "internal market for personal data" but also promote commercial relations between the EU and third

countries. The objectives are clear: enhance individuals' rights in data collection and processing, reduce bureaucracy for businesses, and ensure high data protection standards for cross-border data flows.

As mentioned above, the European Regulation establishes the possibility for the Commission or the supervisory authority to adopt standard contractual clauses regulating the obligations, for data protection purposes, between the controller and the processor, on which the contracts entered into between the controller and the processor may be based. However, it will be necessary to await the development of these clauses by the Commission or supervisory authority in order to determine whether it is more appropriate to draw up ad hoc clauses or to adhere to the standard clauses.

The international transfer of personal data is possible as a result of the implementation of one of the following European Commission Decisions. Depending on the purpose or legal framework in which they are carried out, international transfers can be categorised as contractual (international transfers as a consequence of contractual and commercial relations between companies with legal links or the flow maintained for commercial purposes), resulting from prior agreements between data exporters and importers, or non-contractual (unlawful

processing of data)[15], when there is no such agreement.

Among the criteria set out above, for the purposes of private international law, the one that interests in this paper - addressing the lack of protection of the holder of the right to data protection derived from an unlawful international transfer of personal data - is the purpose or legal framework in which the transfer is carried out. This distinction enables the classification of international data transfers as either contractual (consensual) or non-contractual (non-consensual).

The former ("contractual" international data transfers) refer to international data processing transactions between the data subject and the controller. It is frequent that the conclusion or execution of a certain agreement between a data subject and an employer (or between the latter and a third party in the interest of the former) requires the processing of his personal data. In such cases, the international transfer of such data is ancillary to the main business. In other cases, the international transfer of data takes place within the framework of a business whose main purpose is precisely that transfer: these are transfers of data that take place on a principal basis.

In addition to these cases, there are instances of data subjects' data protection rights being infringed due to unauthorised data processing carried out by an employer outside a pre-existing

15Consequently, there will be damage - and therefore a claim - if it is established that there has been unlawful processing of personal data.

relationship between the parties ("extra-contractual" international data transfers), where the data subject (injured party) brings a claim for damages against the tortfeasor (the natural or legal person who has unlawfully processed the data).

Conclusions

The GDPR is based on the criteria already established in Directive 95/46 and incorporated into Spanish domestic legislation. It stipulates that data may only be transferred to those countries, territories, sectors or international organisations for which the European Commission has considered that they have an adequate level of protection or, in other cases, sufficient guarantees are provided or some of the circumstances foreseen as exceptions are met, and provided that the other requirements of the Regulation are observed.

The GDPR introduces new features that affect the entire international transfer regime, but it is the authorisation regime that represents a radical departure from the model of the current regulation. The first issue is that the GDPR establishes beyond doubt that the data exporter can be both a controller and a processor, a precision that definitively puts an end to the legal restrictions in certain Member States where the exporter must always be the controller. This means that service providers established in third countries are in a better position to

subcontract in those or other third countries than service providers established in the EU. The Spanish Data Protection Agency has already addressed this by adopting model contractual clauses that offer sufficient guarantees for international transfers from Spanish processors to sub-processors in third countries.

It also broadens the range of instruments in which appropriate safeguards can be included and provided to protect the rights of data subjects as a result of the transfer of data. Codes of conduct and certification mechanisms are incorporated as instruments that can incorporate these guarantees. In addition to the Binding Corporate Rules (BCRs) for multinational groups which, although in practice they are already operational, thanks to the work of the Article 29 Working Party (WP29), for the first time they are recognised with legal status. This will make their use possible in those Member States that to date do not consider them valid, as they derive their binding effect not only from contracts but also from unilateral declarations. This wider range of instruments should facilitate the work of exporters by giving them more to choose from.

But where the new features introduced by the GDPR are most evident is in the regime of prior authorisation and notification of international transfers, which are reduced to very few cases. The current applicable regulations oblige data exporters to request

prior authorisation from the Spanish Data Protection Agency in order to transfer data to importers established in countries that do not have an adequate level of protection, provided that they provide sufficient guarantees. They also had to notify the agency when transferring data to countries with adequate protection or when specific exceptions in Article 34 of the Organic Law on Data Protection were applied. Under the GDPR, transfers may be carried out without the need for prior authorisation, unless the guarantees are provided through an ad hoc contract or an administrative agreement between public authorities, or notification to the supervisory authority. There is an exception based on the overriding legitimate interest of the controller, but this too has specific requirements outlined in the GDPR.

These substantive changes will undoubtedly facilitate trade relations and international cooperation by avoiding the need to seek authorisation from the Agency in most cases, but at the same time guaranteeing the rights of data subjects when data is transferred outside the EU.

References

Aced Fèlez, E. (2005). Transferencias internacionales de datos. In Piñar Mañas, J. L. (Dir.). *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 June 2003).* Tirant lo Blanch, Valencia, 108-109.

Estadella Yuste, O. (1996). *La transmisión internacional de datos personales y su control.* Jornadas sobre Derecho Español de Protección de Datos Personales, Agencia de Protección de Datos, Madrid, 202.

Fernàndez Lòpez, J.M. (February 2007). Movimiento internacional de datos y buen gobierno corporativo. *Boletín del Ilustre Colegio de Abogados de Madrid, núm. 35,* 177.

Garriga Domìnguez, A. (1999). *La protección de los datos personales en el Derecho español.* Dykinson, Madrid, 331.

Guasch Portas, V. (2014). *Las transferencias internacionales de datos en la normativa española y comunitaria.* Agencia Española de Protección de Datos-Agencia Estatal Boletín Oficial del Estado, Madrid.

Herràn Ortiz, A.I. (2002). *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales.* Dykinson, Madrid, 368.

Lòpez Carballo, D. (2016). A vueltas con las transferencias internacionales de datos: actualidad y seguridad jurídica.

Actualidad Jurídica Aranzadi, núm. 922/2016, Aranzadi, Cizur Menor (Navarra).

Ortega Gimènez, A. (March 2018). El Reglamento General de Protección de Datos de la UE en la empresa: novedades prácticas. *Diario La Ley, 15,* Section Ciberderecho, Editorial Wolters Kluwer.

Ortega Gimènez, A., Gonzalo Domenech, J.Josè (February 2018). Las transferencias internacionales de datos de carácter personal en el nuevo Reglamento General de Protección de Datos. *iRevista Economist & Jurist, Number 217, Difusión Jurídica,* 36-43.

Ortega Gimènez, A. (January 2018). Impacto del nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea: del "safe harbour" al "privacy shield", *Revista Digital Administrativo, Editorial jurídica Sepin, Nº 24,* SP/DOCT/73156, Monographic Article.

Ortega Gimènez, A. (2017). *El nuevo régimen jurídico de la Unión Europea para las empresas en materia de protección de datos de carácter personal.* Cizur Menor (Navarra): Thomson Reuters Aranzadi.

Ortega Gimènez, A. (2016). *Transferencias internacionales de datos de carácter personal ilícitas.* Cizur Menor (Navarra): Thomson Reuters Aranzadi.

Ortega Gimènez, A. (2015). La (des) protección del titular del

derecho a la protección de datos derivada de una transferencia internacional ilícita en Derecho internacional privado español. *Diario La Ley, Nº 8661*, La Ley, Madrid.

Ortega Gimènez, A. (2015). *La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita.* AEPD, Madrid.

Ortega Gimènez, A., Marzo Portera, A. (2013): E*mpresa y transferencia internacional de datos personales.* Instituto Español de Comercio Exterior (ICEX), Madrid.

Ortega Gimènez, A. (2013). Imagen y circulación internacional de datos. *Revista Boliviana de Derecho, No. 15,* Fundación Iuris Tantum, Santa Cruz (Bolivia).

Piñar Mañas, J.L. (Dir.) (2005). *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 June 2003).* Tirant lo Blanch, Valencia, 108-109.

Sancho Villa, D. (2010). *Negocios Internacionales de Tratamiento de Datos Personales.* Cizus Menor Civitas, Navarra.

Sancho Villa, D. (2003). *Transferencia internacional de datos personales*. Agencia de Protección de Datos, Madrid.

Solar Calvo, P. (2012). La doble vía europea en protección de datos. *Diario La Ley, Nº 7832,* Doctrina Section, Editorial La Ley.

Villarino Marzo, J. (2013). La privacidad desde el diseño en la propuesta de reglamento europeo de protección de datos. *Revista Aranzadi de Derecho y Nuevas Tecnologías núm. 32/2013,* Aranzadi, Cizur Menor.